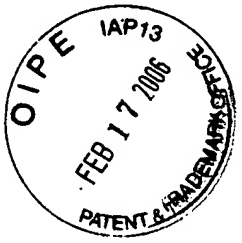
AF/ZFW

Sterne Kessler Goldstein Fox
ATTORNEYS AT LAW



Robert Greene Sterne
Jorge A. Goldstein
David K.S. Cornwell
Robert W. Esmond
Tracy-Gene G. Durkin
Michele A. Cimbala
Michael B. Ray
Robert E. Sokohl
Eric K. Steffe
Michael Q. Lee
Steven R. Ludwig
John M. Covert
Linda E. Horner
Robert C. Millonig
Donald J. Featherstone
Timothy J. Shea, Jr
Michael V. Messinger
Judith U. Kim

Patrick E. Garrett
Jeffrey T. Helvey
Heidi L. Kraus
Eldora L. Ellison
Thomas C. Fiala
Donald R. Banowit
Peter A. Jackman
Jeffrey S. Weaver
Brian J. Del Buono
Vincent L. Capuano
Virgil Lee Beaston
Theodore A. Wood
Elizabeth J. Haanes
Joseph S. Ostroff
Frank R. Cottingham
Rae Lynn P. Guest
Daniel A. Klein
Jason D. Eisenberg

Michael D. Specht
Tracy L. Muller
Jon E. Wright
LuAnne M. DeSantis
Ann E. Summerfield
Helene C. Carlson
Cynthia M. Bouchez
Timothy A. Doyle
Gaby L. Longsworth
Lori A. Gordon
Ted J. Ebersole
Laura A. Vogel
Bryan S. Wade
Bashir M.S. Ali
Shannon A. Carroll
Matthew E. Kelley
Michelle K. Holoubek•
Marsha A. Rose•

W. Blake Coblentz*
James J. Pohl*
John T. Haran*
Mark W. Rygiel

Registered Patent Agents•
Karen R. Markowicz
Matthew J. Dowd
Katrina Yujian Pei Quach
Bryan L. Skelton
Robert A. Schwartzman
Teresa A. Colella
Victoria S. Rutherford
Simon J. Elliott
Julie A. Heider
Mita Mukherjee
Scott M. Woodhouse
Christopher J. Walsh

Liliana Di Nola-Baron
Peter A. Socarras
Jeffrey Mills
Danielle L. Letting
Lori Brandes

Of Counsel
Edward J. Kessler
Kenneth C. Bass III
Marvin C. Guthrie

*Admitted only in Maryland
*Admitted only in Virginia
•Practice Limited to Federal Agencies

February 17, 2006

WRITER'S DIRECT NUMBER:
(202) 772-8862
INTERNET ADDRESS:
LGORDON@SKGF.COM

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Art Unit 2164

Attn: Mail Stop Appeal Brief - Patents

Re: U.S. Utility Patent Application
Application No. 09/610,798; Filed: July 6, 2000
For: **Distributed Processing in a Cryptography Acceleration Chip**
Inventors: KRISHNA *et al.*
Our Ref: 1875.4310003

Sir:

Transmitted herewith for appropriate action are the following documents:

1. Reply to Notification of Non-Compliant Appeal Brief;
2. Amended Brief on Appeal Under 37 C.F.R. §41.37
3. One (1) Return postcard.

It is respectfully requested that the attached postcard be stamped with the date of filing of these documents, and that it be returned to our courier. In the event that extensions of time are necessary to prevent abandonment of this patent application, then such extensions of time are hereby petitioned.

The U.S. Patent and Trademark Office is hereby authorized to charge any fee deficiency, or credit any overpayment, to our Deposit Account No. 19-0036.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

RES/LAG:smn
Enclosures

497977_1.DOC

OIPE IAP13 FEB 17 2006 PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 4877
KRISHNA *et al.*	Art Unit: 2164
Application No.: 09/610,798	Examiner: Ortiz, Belix M.
Filed: July 6, 2000	Atty. Docket: 1875.4310003
For: **Distributed Processing in a Cryptography Acceleration Chip**	

Reply to Notification of Non-Compliant Appeal Brief

Attn: Mail Stop Appeal Brief - Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In reply to the Notification of Non-Compliant Appeal Brief, Appellants submit the following Amended Appeal Brief and Remarks. The required brief filing fee of $500.00 under 37 C.F.R. § 41.20(b)(2) for a large entity was submitted with Appellants' filing on November 15, 2005. It is not believed that any additional fees are required. However, if additional fees are necessary to prevent abandonment of this application, then such are hereby authorized to be charged to our Deposit Account No. 19-0036.

Remarks

The Notification of Non-Compliant Appeal Brief states that Appellants' Brief filed on November 15, 2005 did "not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading, or in the proper order." Appellants respectfully disagree with this statement. Appellants' Brief included all required sections under 37 CFR 41.37(c), under the proper heading, and in the proper order. *See* Appeal Brief, Table of Contents. Appellants' Appeal Brief included an extra section entitled "Background" between the "Status of Amendments (37 C.F.R. §41.37(c)(1)(v))" and "Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(vi))" sections. The Background section provides additional information to aid in the understanding of Appellants' claimed invention. Appellants submit that the inclusion of this section does not cause the Appeal Brief to be defective. However, to expedite consideration of the Brief, Appellants have amended the Brief to incorporate the Background section into the "Status of Amendments (37 C.F.R. §41.37(c)(1)(v))" section. *See* Amended Appeal Brief.

The Notification of Non-Compliant Appeal Brief further states that the Brief "does not contain a statement of the status of all claims ... or does not identify the appealed claims." Specifically, the Examiner states that the "'Status of Claims' section must clearly identify all claims status at the time of final rejection and which one are on appeal." In response, Appellants have added the following statement to the "Status of Claims" section.

> At this time of the final rejection, claims 24-41 stand rejected. Accordingly, claims 24-41 are on appeal. A copy of the claims on appeal can be found in the Claims Appendix section.

The Notification of Non-Compliant Appeal Brief further states that "[a]t least one amendment has been filed subsequent to the final rejection, and the brief does not contain a statement of the status of each such amendment." Appellants respectfully disagree with this statement. Appellants have not filed an amendment subsequent to the final rejection. On August 2, 2005, Appellants filed a reply to the final Office Action dated June 2, 2005. The reply included no amendments to the claims. To expedite consideration of the Brief, Appellants have added the following statement to the "Status of Amendments" section:

> On August 2, 2005, a reply to the final Office Action dated June 2, 2005 was filed. The reply included no claim amendments.

In addition, Appellants corrected a typographical error in the Application Number in the header of the Appeal Brief. Accordingly, all of the stated grounds of non-compliance have been properly traversed, accommodated, or rendered moot. Appellants therefore respectfully request that the attached Amended Appeal Brief be entered.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon

Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: February 17, 2006

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

OIPE IAP13
FEB 17 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: KRISHNA *et al.*	Confirmation No.: 4877
Application No.: 09/610,798	Art Unit: 2164
Filed: July 6, 2000	Examiner: Ortiz, Belix M.
For: **Distributed Processing in a Cryptography Acceleration Chip**	Atty. Docket: 1875.4310003

Amended Brief on Appeal Under 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal from the final rejection of claims 24-32 and 36-41 and the objection to claims 33-35 was filed on September 15, 2005. Appellants hereby file one copy of this Amended Appeal Brief. The required fee set forth in 37 C.F.R. §41.20(b)(2) was submitted with Appellants' Appeal Brief filing on November 15, 2005.

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to our Deposit Account No. 19-0036.

OIPE IAP13 FEB 17 2006 PATENT & TRADEMARK OFFICE

Table of Contents

I. Real Party In Interest (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest is Broadcom Corporation, having its principal place of business at 16215 Alton Parkway, Irvine, California, 92618-3636. An assignment assigning all right, title, and interest in and to the patent application from the inventors to Broadcom was recorded in the U.S. Patent & Trademark Office on November 6, 2000 at Reel 011224, Frame 0283.

II. Related Appeals and Interferences (37 C.F.R. § 41.37(c)(1)(ii))

To the best knowledge of Appellants, Appellants' legal representative, and Appellants' assignee, there are no other appeals or interferences which will directly affect or be directly affected or have a bearing on a decision by the Board of Patent Appeals and Interferences ("the Board") in the pending appeal.

III. Status of Claims (37 C.F.R. § 41.37(c)(1)(iii))

The application was originally filed as U.S. Application 09/610,798 on July 6, 2000 with 23 claims (numbered 1-18 and 20-24). In the preliminary amendment filed on November 2, 2000, Appellants renumbered claims 20-24 as claims 19-23 and updated their dependencies to correct for an error in numbering the original claim set (claim number 19 skipped). In the Amendment and Reply filed on July 2, 2004, Appellants canceled claims 1-23 and added claims 24-41.

The pending claims were finally rejected in an Office Action mailed June 2, 2005. The Advisory Action mailed on August 12, 2005 stated that the Reply filed on August 2, 2005 did not place the application in condition for allowance. At this time of the final rejection, claims 24-41 stand rejected. Accordingly, claims 24-41 are on appeal. A copy of the claims on appeal can be found in the Claims Appendix section.

IV. Status of Amendments (37 C.F.R. § 41.37(c)(1)(iv))

All amendments have been entered. The Office Action dated December 30, 2004, responded to and acknowledged Appellants' amendment filed July 2, 2004. Thus, claims 24-41 are currently pending in the application. On August 2, 2005, a reply to the final Office Action dated June 2, 2005 was filed. The reply included no claim amendments.

V. Summary of Claimed Subject Matter (37 C.F.R. § 41.37(c)(1)(v))

The claimed invention relates generally to the field of cryptography, and more particularly to an architecture and method for distributed processing in a cryptography acceleration chip. Many methods for performing cryptography are well known in the art. In order to improve the speed of cryptography processing, specialized cryptography accelerator chips have been developed. Cryptography accelerator chips may be included in routers or gateways, for example, in order to provide automatic IP packet encryption/decryption. By embedding cryptography functionality in network hardware, both system performance and data security are enhanced. (Specification, p. 1, lines 19-27).

However, these prior cryptography acceleration chips have limitations. Many of these prior acceleration chips require sizeable external attached memory in order to operate. (Specification, p. 1, lines 28-31). Also, the actual sustained performance of these chips is much less than peak throughput than the internal cryptography engines (or "crypto engines") can sustain. One reason for this is that the chips have a long "context" change time. In other words, if the cryptography keys and associated data need to be changed on a packet-by-packet basis, the prior chips must swap out the current context and load a new context, which reduces the throughput. (Specification, p.2, lines 1-8). Moreover, the architecture of prior chips does not allow for the processing of

cryptographic data at rates sustainable by the network infrastructure in connection with which these chips are generally implemented. This can result in noticeable delays when cryptographic functions are invoked, for example, in e-commerce transactions. (Specification, p. 2, lines 9-12).

FIG. 2 of the Specification, reprinted below, illustrates an exemplary high-level block diagram of a cryptography system, in accordance with the subject matter claimed. Independent claim 24 is directed to a system including a distributor unit 206 and a plurality of security processing engines 214. (Specification, FIG. 2, reproduced below).

Distributor unit 206 distributes the packet data and the security association information (SA) received from, for example, packet classifier unit 204 among a plurality of security processing engines 214 for security processing. (Specification, p. 8, lines 19-23). Thus, the distributor 206 hands off a parallelizable portion of security processing to the security processing engines. (Specification, p. 9, lines 10-11). By providing multiple security processing engines and processing data packets in parallel, systems in accordance with the present invention are able to provide greatly improved security processing performance. (Specification, p. 9, lines 11-13).

Security processing is performed on a plurality of the received packets in parallel by the security processing engines 214. (Specification, p. 9, lines 11-12). Security processing engines 214 may perform, for example, encryption/decryption, authentication/digital signature processing and compression/decompression processing. (Specification, p. 9, lines 24-26).

The system also includes various buffers 210 for storing packet data, security association information, status information, etc. For example, packets may be stored in packet buffers and security association information may be may be stored in context or security association buffers. (Specification, p. 10, lines 25-29).

The system also includes a packet classifier unit 204. The packet classifier unit 204 receives packet header information for packets to be processed. (Specification, p. 8, lines 8-9). Classification engine 204 then determines security association information required for processing the packet, such as encryption keys, data, etc. (Specification, p. 8, lines 9-10). In an exemplary embodiment, the classification engine performs lookups from databases stored in associated memory. The security association information determined by the packet classifier unit 204 is sent to a packet distributor unit 206. (Specification, p. 8, lines 17-18).

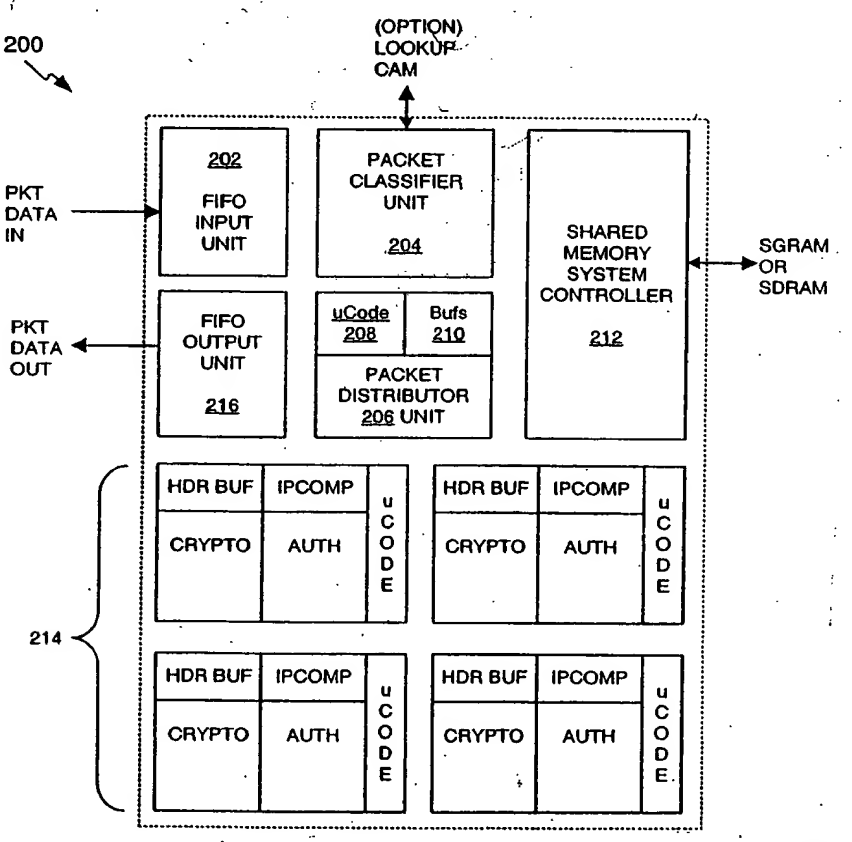


FIG. 2

VI. Grounds of Rejection to be Reviewed on Appeal (37 C.F.R. § 41.37(c)(1)(vi))

In the final Office Action mailed June 2, 2005, claims 24-26 and 36-41 were rejected under 35 U.S.C. §102(e) as being anticipated by Gunter, et al, U.S. Patent No. 6,751,728 (Gunter). Claim 27 was rejected under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Barlow, et al, U.S. Patent No. 6,038,551 (Barlow) and claims 28-32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Leung, U.S. Patent No. 6,760,444 (Leung). Claims 33-35 were objected to as being dependent upon a rejected base claim.

Accordingly, the grounds of rejection and objections to be reviewed on appeal are:

A. Rejection of claims 24-26 and 36-41 under 35 U.S.C. §102(e) as being anticipated by Gunter.

B. Rejection of claim 27 under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Barlow.

C. Rejection of claims 28-32 under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Leung.

D. Objection to claims 33-35 as being dependent upon a rejected base claim.

VII. Argument (37 C.F.R. § 41.37(c)(1)(vii))

A. Ground A. Rejection of claims 24-26 and 36-41 under 35 U.S.C. §102(e) as being anticipated by Gunter.

1. The Examiner's Anticipation Rejection

A Final Office Action was mailed on June 2, 2005, rejecting claims 24-26 and 36-41 under U.S.C. §102(e) as being anticipated by Gunter. Appellants' remarks focus

mainly on independent claim 24, because any claim which depends from a patentable independent claim is also patentable by virtue of its dependency.

2. The Anticipation Rejection is in Error and Must be Reversed

To establish a *prima facie* case of anticipation under §102(a), the Examiner must show that "each an every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). Because the Examiner has failed to establish that each and every element is described in Gunter, the rejection of claims 24-26 and 36-41 must be reversed.

Gunter does not teach all the elements of Appellants' independent claim 24. Specifically, Gunter does not teach or suggest "a distributor unit that distributes a plurality of packets and security information associated with the plurality of packets according to a distribution scheme," as recited in independent claim 24. In response to Appellants' arguments in the Reply filed on March 29, 2005, the Examiner states:

> Gunter et al. teaches a plurality of packets and security associated information associated with the plurality of packets in "A method and system for network communication efficiently transmits encrypted packets from a sending host on an external network to a receiving host on an intranet through a network access point (NAP) of the intranet. A packet to be sent by the sending host on the external network is constructed with the external network address of the NAP as the destination address of the packet. The intranet address of the receiving host is also included in the packet in the non-encrypted form and is used in the calculation of the cryptographic hash or the like that is included in the packet for authentication purposes."

(Final Office Action mailed June 2, 2005, p. 8, citing Gunter, col. 1, lines 62-65 and col. 2, lines 36-40)(emphasis in original). The Examiner appears to be equating the sending host of Gunter with the distributor unit recited in Appellants' claim 24 and the destination address of the packet, the intranet address of the receiving host, and the calculated cryptographic hash with security association information recited in Appellants' claim 24.

None of the elements of the packet described in Gunter, including those listed by the Examiner, are security association information. The Examiner simply misunderstands the term "security association information," as used in the cryptographic arts.

A security association is an agreement between two communicating entities that defines information necessary to perform security processing on an in-bound or out-bound IP packet exchanged between the entities. Appellants' specification describes security association information and its use:

> The IPSec cryptography protocol specifies two levels of lookup: Policy (Security Policy Database (SPD) lookup) and Security Association (Security Association Database (SAD) lookup). The policy look-up is concerned with determining what needs to be done with various types of traffic, for example, determining what security algorithms need to be applied to a packet, without determining the details, e.g., the keys, etc. The Security Association lookup provides the details, e.g., the keys, etc., needed to process the packet according to the policy identified by the policy lookup."

(Specification, p. 11, line 33 - p. 12, line 4). Furthermore, the terms "security association" and "security association information" were well-known in the art at the time the '798 application was filed. For example, Internet Engineering Task Force (IETF) Request for Comment (RFC) 2401, entitled "Security Architecture for the Internet Protocol" which was incorporated by reference in its entirety into the '798 application, describes exemplary security association information stored in a security association database. As described in RFC 2401, security association information includes a sequence number counter, anti-replay window, authentication header (AH) authentication algorithm and keys, encapsulated security protocol (ESP) authentication algorithm and keys, ESP encryption algorithm, keys, initialization vector mode, and initialization vector, and security association lifetime. (Kent, "Security Architecture for the Internet Protocol," RFC 2401, p. 21). Based on the foregoing, it is readily apparent that security

association information is information that is used to perform security association on packets, including encrypted portions of a packet.

In Gunter, the packet exchanged between a sending host and a network access point (NAP) does not include security association information. As shown in FIG. 7, the packet in Gunter includes a source address 108, the NAP address (destination address) 110, data 112, cryptographic hash value 116, and the receiving host intranet address 126. (Gunter, FIG. 7). Source address 108, destination address 110, and receiving host intranet address 126 are not security association information. At most, one or more of these fields can be used as selectors to access security association information. (Specification, p. 13, lines 11-23). Similarly the cryptographic hash value 116 is not security association information. The hash value provides no information needed to perform security processing on the packet. It is simply additional data included in the payload of the packet.

Furthermore, Gunter teaches away from the distribution of security association information associated with each of the plurality of packets by the sending host. Specifically, Gunter states "the data portion 112 and the cryptographic hash 116 are then encrypted using a known encryption mechanism ... encryption may use a single key known to both the sending and receiving hosts or the public private key scheme." (Gunter, col. 7, lines 45-50). Gunter therefore teaches that the sending and receiving hosts store the information needed for security processing locally (e.g., encryption protocol identification, authentication (hash) protocol identification, and encryption keys). In Gunter, there is no need to distribute security association information from a sending host to a NAP or from a NAP to a receiving host because the information necessary for security processing is stored locally at the hosts and/or NAP.

Furthermore, Gunter does not teach or suggest "wherein the plurality of security processing engines receive at least a portion of the security association information associated with the packets, and wherein the plurality of security processing engines process the plurality of packets in parallel," as recited in independent claim 24. In response to Appellants' arguments filed on March 29, 2005, the Examiner states:

> Gunter et al. teaches wherein the plurality of security processing engines receive at least a portion of the security association information associated with the packets, and wherein the plurality of security processing engines process the plurality of packets in parallel on "When the receiving host receives the modified packet, it decrypts the encrypted portion and authenticates the packet by calculating another hash value based on the addresses and data in the received packet, and comparing this hash value with the hash value included in the packet."

(Final Office Action mailed June 2, 2005, p. 9, citing Gunter, col. 2, lines 4-9 and col. 2, lines 36-50)(emphasis in original).

In further support of the rejection, the Examiner uses the following passages of Gunter:

> When the receiving host receives the modified packet, it decrypts the encrypted portion and authenticates the packet by calculating another hash value based on the addresses and data in the received packet, and comparing this hash value with the hash value included in the packet. (Gunter, Col. 2, lines 4-9).
>
> Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, game port or a universal serial bus (USB). (Gunter, Col. 4, lines 31-35).

(Final Office Action mailed June 2, 2005, p. 3). In this rejection, the Examiner appears to be disregarding the exact language used in claim 24. This is not allowable. When making a determination as to the patentability of a claim, "[a]ll words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). None of the passages of Gunter

cited by the Examiner teach or suggest that "the plurality of security processing engines receive at least a portion of the security association information associated with the packets" or that "the plurality of security processing engines process the plurality of packets in parallel."

Gunter simply does not teach or suggest the distribution of security association information to a plurality of security processing engines or the processing of a plurality of packets in parallel by the plurality of security processing engines. Gunter at most describes security processing performed by a single receiving host. The discussion by Gunter of the use of a parallel port to couple an input device to a processing unit is wholly unrelated to parallel processing of a plurality of packets.

As described above, Gunter does not teach or suggest each and every limitation of independent claim 24. Therefore, independent claim 24 is patentable over Gunter. Furthermore, for at least these reasons and further in view of their own features, claims 25, 26, and 36-41 which depend from claim 24 are patentable over Gunter.

In addition, Gunter does not teach or suggest "wherein the plurality of packets are buffered prior to being processed by the plurality of security processing engines," as recited in Appellants' dependent claim 25. In support of this rejection, the Examiner cites a passage from Gunter describing BIOS. (Final Office Action mailed June 2, 2005, p. 3). The discussion of BIOS is wholly unrelated to buffering of packets. For at least this further reason, claim 25 is patentable over Gunter.

Gunter also does not teach or suggest "a classification module that determines security association information associated with a plurality of packets, wherein the classification module is configured to provide at least a portion of the security information associated with the packets to the distributor unit," as recited in Appellants' dependent claim 26. In support of this rejection, the Examiner cites passages from the

claims related to the construction of the packet by the sending host (Final Office Action mailed June 2, 2005, p. 3). As discussed above, none of the elements of the packet constructed by the sending host in Gunter are security association information. Furthermore, Gunter does not teach a classification module that determines security association information associated with a plurality of packets. For at least this further reason, dependent claim 26 is patentable over Gunter.

For at least the foregoing reasons, claims 24-26 and 36-41 are patentable over Gunter and the rejection of claims 24-26 and 36-41 must be reversed.

B. Ground B. Rejection of claim 27 under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Barlow.

1. The Examiner's Obviousness Rejection

A Final Office Action was mailed on June 2, 2005, rejecting claim 27 under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Barlow.

2. The Obviousness Rejection is in Error and Must be Reversed.

Claim 27 depends from claim 24. Barlow does not overcome all of the deficiencies of Gunter relative to claim 24, described above. For at least this reason and further in view of its features, claim 27 is patentable over Gunter. Therefore, the rejection of claim 27 is in error and must be reversed.

C. Ground C. Rejection of claims 28-32 under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Leung.

1. The Examiner's Obviousness Rejection

A Final Office Action was mailed on June 2, 2005, rejecting claims 28-32 under 35 U.S.C. §103(a) as being unpatentable over Gunter in view of Leung.

2. The Obviousness Rejection is in Error and Must be Reversed.

Claims 28-32 depend from claim 24. Leung does not overcome all of the deficiencies of Gunter relative to claim 24, described above. For at least this reason and further in view of their own features, claims 28-32 are patentable over Gunter. Therefore, the rejection of claims 28-32 is in error and must be reversed.

D. Ground D. Objection to claims 33-35 as being dependent upon a rejected base claim.

1. The Examiner's Objection

A Final Office Action was mailed on June 2, 2005, objecting to claims 33-35 as being dependent upon a rejected base claim.

2. The Objection is in Error and Must be Reversed.

Claims 33-35 depend from claim 24. As described above, claim 24 is patentable over Gunter. For at least this reason, the objection to claims 33-35 as being dependent upon a rejected base claim must be reversed.

VIII. Conclusion

Claims 24-26 and 36-41 are patentable over Gunter because the Examiner has failed to establish that Gunter anticipates claims 24-26 and 36-41. Claim 27 is patentable over the combination of Gunter and Barlow and claims 28-32 are patentable over the combination of Gunter and Leung because the Examiner has failed to make a *prima facie* case of obviousness. Therefore, Appellants respectfully request that the Board reverse the Examiner's final rejection of these claims, the objection to claims 33-35, and remand this application for issue.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Lori A. Gordon

Lori A. Gordon
Attorney for Applicants
Registration No. 50,633

Date: February 17, 2006

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

IX. Claims Appendix (37 C.F.R. § 41.37(c)(1)(viii))

1-23. (canceled)

24. (previously presented) A system, comprising:

a distributor unit that distributes a plurality of packets and security association information associated with the plurality of packets according to a distribution scheme; and

a plurality of security processing engines, coupled to the distributor unit, that perform authentication and cryptographic functions,

wherein the plurality of security processing engines receive at least a portion of the security association information associated with the packets, and wherein the plurality of security processing engines process the plurality of packets in parallel.

25. (previously presented) The system of claim 24, wherein the plurality of packets are buffered prior to being processed by the plurality of security processing engines.

26. (previously presented) The system of claim 24, further comprising a classification module that determines security association information associated with a plurality of packets, wherein the classification module is configured to provide at least a portion of the security information associated with the packets to the distributor unit.

27. (previously presented) The system of claim 24, wherein the distributor unit and the plurality of security processing engines are on the same chip.

28. (previously presented) The system of claim 24, wherein the security association information includes a sequence number, an anti-replay window, and a lifetime of the security association.

29. (previously presented) The system of claim 28, wherein the security association information further includes an encapsulating security payload (ESP) encryption algorithm identifier and one or more ESP encryption keys.

30. (previously presented) The system of claim 29, wherein the security association information further includes an ESP authentication algorithm identifier and one or more ESP authentication keys.

31. (previously presented) The system of claim 28, wherein the security association information further includes an authentication header (AH) authentication algorithm identifier and one or more AH authentication keys.

32. (previously presented) The system of claim 28, wherein the security association information includes protocol mode information.

33. (previously presented) The system of claim 24, wherein the distribution scheme is a round-robin distribution scheme, wherein the distributor unit selects a next available security processing engine in a round-robin manner.

34. (previously presented) The system of claim 24, further comprising an order maintenance packet retirement unit.

35. (previously presented) The system of claim 34, wherein the distributor unit assigns packets for processing to a next available security processing engine regardless

of the order received and the order maintenance packet retirement unit outputs the processed packets such that packet order is maintained.

36. (previously presented) The system of claim 24, wherein the system is a router.

37. (previously presented) The system of claim 24, wherein the system is a firewall.

38. (previously presented) The system of claim 24, wherein the system is a network communication device.

39. (previously presented) The system of claim 24, wherein the system is a security gateway.

40. (previously presented) The system of claim 24, wherein the system is a server.

41. (previously presented) The system of claim 24, wherein the system is a network line card.

X. Evidence Appendix (37 C.F.R. § 41.37(c)(1)(ix))

None

XI. Related Proceedings Appendix (37 C.F.R. § 41.37(c)(1)(x))

None